UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/457,914	12/10/1999	GERMANO CARONNI	06502.0289	8208

22852 7590 04/22/2005

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/457,914	CARONNI ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5,7-11,13-20,22,24-31,33-37,39 and 41-48* is/are pending in the application.

4a) Of the above claim(s) *4,6,12,21,23,32,38 and 40* is/are ~~withdrawn from consideration~~ Canceled.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5,7-11,13-20,22,24-31,33-37,39 and 41-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10 IDS*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39, and 41-45 have been re-examined and maintains the rejection in view of Devine, et al. Therefore this is a Final rejection.

Applicant have amended independent claims 1, 16, 18, 29, 33, and 35,

Applicant have added claims 46-48.

Applicant have cancelled claims 4, 6, 12, 21, 23, 32, 38, and 40.

2. Claims 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39, and 41-48 contains new subject matter and have been rejected under 35 U.S.C. 112, 1st paragraph.

3. Claims 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39, and 41-48 have been rejected under 35 U.S.C. 102(e).

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39, and 41-48 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 1, 16, 18, 29, 33, and 35 contains new matter issues wherein the specification fails to support "without passing through the private network" as amended by Applicant. All other claims are also rejected that are dependent onto the rejected claims above.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39, and 41-48 are rejected under 35 U.S.C. 102(e) as being anticipated by Devine, et al. (US 6,606,708).

As per claim 1:

Devine, et al. teaches a method executed in a data processing system for providing communication access between a first process associated with a first node and a second process associated with a second node, the method comprising:

sending a request from the first node to a server associated with a private network to verify a first node identification associated with the first process; **(col.8, lines 23-30)**

in response to the request, receiving security context information at the first node from the server, the security context information comprising a virtual address for the first node; **(col.13, lines 40-47 and col.23, lines 27-28)**

appending the security context information for the first process in a process table; **(col.9, lines 60-63, col.13, lines 60-67)**

opening a socket between the first process and the second process; and **(col.8, lines 22-26)**

transmitting a packet from the first process to the second process through the open socket without passing through the private network **(col.6, lines 6-7 and col.24, lines 35-36)**, the packet comprising the security context information for the first process in the process table. **(col.14, lines 6-11)**

As per claim 2: **See col.12, lines 34-37**; discusses modifying a socket structure so as to accept the security context information.

As per claim 3:

Devine discloses receiving the packet at the second process through the socket; **(col.8, lines 33-35)**

verifying the security context information received in the packet; and **(col.11, line 41 thru col.12, line 12)**

permitting use of the packet if the security context information is verified. **(col.9, lines 24-26)**

As per claim 5: **See col.27, line 43 thru col.28, line 5**; discusses comparing the security context information in the received packet and security context information in another process table.

As per claim 6: Cancelled

As per claim 7: **See col.20, lines 53-63 and col.22, lines 25-30;** discusses determining whether the first and second process belong to two different linked channels ; and permitting use of the packet when the different channels are linked. **(col.23, lines 7-11)**

As per claim 8: **See col.24, line 2 and col.26, lines 40-42;** discusses determining whether the first and second process belong to two different linked channels includes initiating a process that spawns two child processes that are connected by a shared-memory region in a memory.

As per claim 9: **See col.8, lines 27-28 and col.12, lines 34--37;** discusses permitting use of the packet includes decrypting the packet on a node and authenticating a sender associated with the first process on the node.

As per claim 10: **See col.9, lines 2-10 and col.14, lines 6-11;** discusses obtaining the security context information from a third process, the security context information comprising a virtual address and a node identification.

As per claim 11: **See col.13, lines 31-67;** discusses modifying a network stack such that the network stack requires the security context information to be present in the socket structure to transmit.

As per claim 12: Cancelled

As per claim 13: **See col.8, lines 52-55;** discusses receiving a key that corresponds to the first node identification from the server.

As per claim 14: See col.9, lines 6-13 and col.13, lines 31-67; discusses encrypting a packet transmitted by the first process using the key; and encapsulating the encrypted packet with a header that comprises the first node identification.

As per claim 15:

Devine teaches a method of claim 1, further comprising:

sending a second request from the second node to the server to verify node identification; **(col.13, lines 49-67)**

receiving additional security context information comprises from the server, wherein the additional security context information includes a second virtual address for the second node; **(col.22, lines 25-30 and col.23, lines 26-28)**

creating the second process; and appending the security context information for the second process in the process table associated with the second process. **(col.8, lines 31-32 and 14, lines 23-30)**

As per claim 16:

Devine teaches a method executed in a data processing system for providing secure communications between a first process associated with a first node and a second process associated with a second node, comprising:

obtaining node identification comprising a virtual address from a server associated with a private network; **(col.23, lines 26-28)**

including the node identification in a field corresponding to the first process in a process table; **(col.13, line 65 thru col.14, line 2)**

transmitting a datagram that contains the node identification the first process to a socket; and **(col.13, lines 60-63)**

receiving the datagram at the second process that contains the node identification and a second virtual address **(col.22, lines 55-56 and col.23, lines 26-28)**, without the datagram passing through the private network. **(col.6, lines 6-7 and col.24, lines 35-36)**

As per claim 17:

Devine teaches the method of claim 16, wherein obtaining a node identification further comprises:

modifying a socket structure in the socket so that the socket structure accepts the node identification; and **(col.13, lines 31-67)**

modifying a process table so that the table comprises a node identification field. **(col.23, lines 26-31 and col.26, lines 24-31)**

As per claim 18:

Devine teaches a system for providing communication access between a first process associated with a first node and second process associated with a second node, comprising:

means for sending a request from the first node to a server associated with a private network to verify a first node identification associated with the first process; **(col.8, lines 23-30)**

means for receiving security context information, in response to the request, at the first node from the server, the security context information

comprising a virtual address for the first node; **(col.13, lines 40-47 and col.23, lines 27-28)**

means for appending security context information for the first process in a process table; **(col.9, lines 60-63, col.13, lines 60-67)**

means for opening a socket between the first process and the second process; and **(col.8, lines 22-26)**

means for transmitting a packet from the first process to the second process through the open socket without passing through the private network **(col.6, lines 6-7 and col.24, lines 35-36)**, the packet comprising the security context information for the first process in the process table. **(col.14, lines 6-11)**

As per claim 19: **See col.12, lines 34-37;** discusses modifying a socket structure so as to accept the security context information.

As per claim 20:

Devine discloses means for receiving the packet at the second process through the socket; **(col.8, lines 33-35)**

means for verifying the security context information received in the packet; and **(col.11, line 41 thru col.12, line 12)**

means for permitting use of the packet if the security context information is verified. **(col.9, lines 24-26)**

As per claim 21: **Cancelled**

As per claim 22: **See col.27, line 43 thru col.28, line 5;** discussing means for comparing the security context information in the received packet and security context information in another process table.

As per claim 23: **Cancelled**

As per claim 24:

Devine discloses the system of claim 20, wherein means for verifying the security context information comprises:

means for determining whether the first and second process belong to two different linked channels; and **(col.20, lines 53-63 and col.22, lines 25-30)**

means for permitting use of the packet when the different channels are linked. **(col.23, lines 7-11)**

As per claim 25: **See col.24, line 2 and col.26, lines 40-42;** discusses means for initiating a process that spawns two child processes that are connected by a shared-memory region in a memory.

As per claim 26: **See col.8, lines 27-28 and col.12, lines 34--37;** discusses means for decrypting the packet on a node; and means for authenticating a sender associated with the first process on the node.

As per claim 27: **See col.9, lines 2-10 and col.23, lines 61-64;** discusses means for obtaining the security context information from a third process including a virtual address and a node identification.

As per claim 28: **See col.13, lines 31-67;** discusses means for modifying a network stack such that the network stack requires the security context information to be present in the socket structure to transmit.

As per claim 29:

Devine teaches a system for placing a process executed in a node in a security context, comprising:

a server associated with a private network; and **(col.6, line 8-9)**

a sending node comprising:

a transmission module that transmit a request to the server to verify a sending node identification **(col.12, lines 36-37)**, and receives security context information from the server in response to the request, wherein the security context information comprises a virtual address for the sending node; **(col.23, lines 26-28 and col.27, lines 47-60)**

memory containing a process and an associated process table; and **(col.13, lines 60-67)**

an appending module that appends the received security context information and the sending node identification for the process in the process table **(col.13, line 43 thru col.14, line 17)**, wherein the transmission module transmits a packet from the process to a receiving node without passing through the private network, the packet comprising the security context information for the first process in the process table. **(col.8, lines 58-59 and col.24, lines 35-36)**

As per claim 30: See col.8, lines 52-55; discusses the transmission module further receives a key that corresponds to the sending node identification from the server.

As per claim 31: See col.9, lines 6-13 and col.13, lines 31-67; discussing an encryption module that encrypts the packet transmitted by the process using the key; and an encapsulating module that encapsulates the encrypted packet with a header that comprises the sending node identification.

As per claim 32: Cancelled

As per claim 33:

Devine teaches a system for providing secure communications between a first process associated with a first node and a second process associated with a second node, comprising:

means for obtaining a node identification comprising a virtual address from a server associated with a private network; **(col.23, lines 26-28)**

means for including the node identification in a field corresponding to the first process in a process table; **(col.13, line 65 thru col.14, line 2)**

means for transmitting a datagram that contains the node identification from the first process to a socket; and **(col.13, lines 60-63)**

means for receiving the datagram at the second process that contains the node identification and a second virtual address **(col.22, lines 55-56 and col.23, lines 26-28)**, without the datagram passing through the private network. **(col.6, lines 6-7 and col.24, lines 35-36)**

As per claim 34:

Devine discloses the system of claim 33, wherein means for obtaining a node identification further comprises:

means for modifying a socket structure in the socket so that the socket structure accepts the node identification; and **(col.13, lines 31-67 and col.14, lines 24-30)**

means for modifying a process table so that the table comprises a node identification field **(col.23, lines 26-31 and col.26, lines 24-31)**

As per claim 35:

Devine discloses a computer readable medium for controlling a data processing system to perform a method for providing communication access between a first process associated with a first node and a second process associated with a second node, comprising:

a sending module for sending a request from the first node to a server associated with a private network to verify a first node identification associated with the first process; **(col.8, lines 23-30)**

a receiving module for receiving security context information, in response to the request, at the first node from the server, the security context information comprising a virtual address for the first node; **(col.13, lines 40-47 and col.23, lines 27-28)**

an appending module for appending security context information for the first process in a process table; **(col.9, lines 60-63, col.13, lines 60-67)**

an opening module for opening a socket between the first process and the second process; and **(col.8, lines 22-26)**

a transmitting module for transmitting a packet from the first process to the second process through the open socket without passing through the private network **(col.6, lines 6-7 and col.24, lines 35-36)**., the packet comprising the security context information for the first process in the process table. **(col.14, lines 6-11)**

As per claim 36: **See col.12, lines 34-37;** discusses modifying module for modifying a socket structure so as to accept the security context information.

As per claim 37:

The computer readable medium for claim 35, further comprising:

a received module for receiving the packet at the second process through the socket; **(col.8, lines 33-35)**

a verifying module for verifying the security context information received in the packet; and **(col.11, line 41 thru col.12, line 12)**

a permitting module for permitting use of the packet if the security context information is verified. **(col.9, lines 24-26)**

As per claim 38: **Cancelled**

As per claim 39: **See col.27, line 43 thru col.28, line 5;** discusses

a comparing module that compares the security context information in the received packet and security context information in another process table.

As per claim 40: **Cancelled**

As per claim 41:

Devine teaches the computer readable medium of claim 37, wherein the verifying module comprises:

a determining module for determining whether the first and second process belong to two different linked channels; and **(col.20, lines 53-63 and col.22, lines 25-30)**

a permitting module for permitting use of the packet when the different channels are linked. **(col.23, lines 7-11)**

As per claim 42: See col.24, line 1 and 26, lines 40-42; discusses determining module comprises a initiating module that initiates a process that spawns two child processes that are connected by a shared-memory region in a memory.

As per claim 43: See col.14, lines 1-2 and col.12, lines 34--37; discusses a decrypting module for decrypting the packet on a node; and an authenticating module for authenticating a sender associated with the first process **(col.8, lines 27-28).**

As per claim 44:

Devine teaches the computer readable medium of claim 35, wherein the appending module comprises:

an obtaining module for obtaining the security context information from a third process, the security context comprising a virtual address and a node identification; and **(col.9, lines 2-10 and col.23, lines 61-64)**

a limiting module for limiting each of the first, second and third processes to communicate with another process provided that the communicating processes share the same node identification. **(col.9, lines 2-10 and col.22, lines 25-30)**

As per claim 45: **See col.13, lines 31-67**; discusses a modifying module for modifying a network stack such that the network stack requires the security context information to be present in the socket structure to transmit.

As per claim 46: **See col.8, lines 31-32 and 14, lines 23-30;** discusses determining if the first and second process belong to a channel; and accepting the transmitted packet when the first and second process belong to the channel.

As per claim 47: **See col.8, lines 31-32 and 14, lines 23-30;** discusses means for determining if the first and second process belong to a channel; and means for accepting the transmitted packet when the first and second process belong to the channel.

As per claim 48: **See col.8, lines 31-32 and 14, lines 23-30;** discusses determining module for determining if the first and second process belong to a channel; and an accepting module for accepting the transmitted packet when the first and second process belong to the channel.

Response to Arguments

Devine discloses communicating from a first node to a server that is associated with a secure network wherein the private network is the secure network of Devine that is within the firewall. Within the firewall or private network is where the request (that contains the security information) and the receiving process occurs. Devine discusses transmitting the packet through the socket without passing through the private network **(col.6, lines 6-7 and col.24, lines 35-36)**. Due to the specification failing to teach or describe the terms "without passing through the private network", the Examiner gives the broadest interpretation which is passing through a public network or the Internet.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100